



QUALYS SECURITY CONFERENCE 2018

# Web Applications & APIs

## Application Security in a Devops world

**Pierrick Prevert**  
Security Solutions Architect

**Remi Le Mer**  
Director of Product Management, WAF

# Agenda

Web Applications & APIs: where are we now ?

Web Security Built-in, not bolted on

Qualys Web Application Scanning

Review | What's New | Roadmap

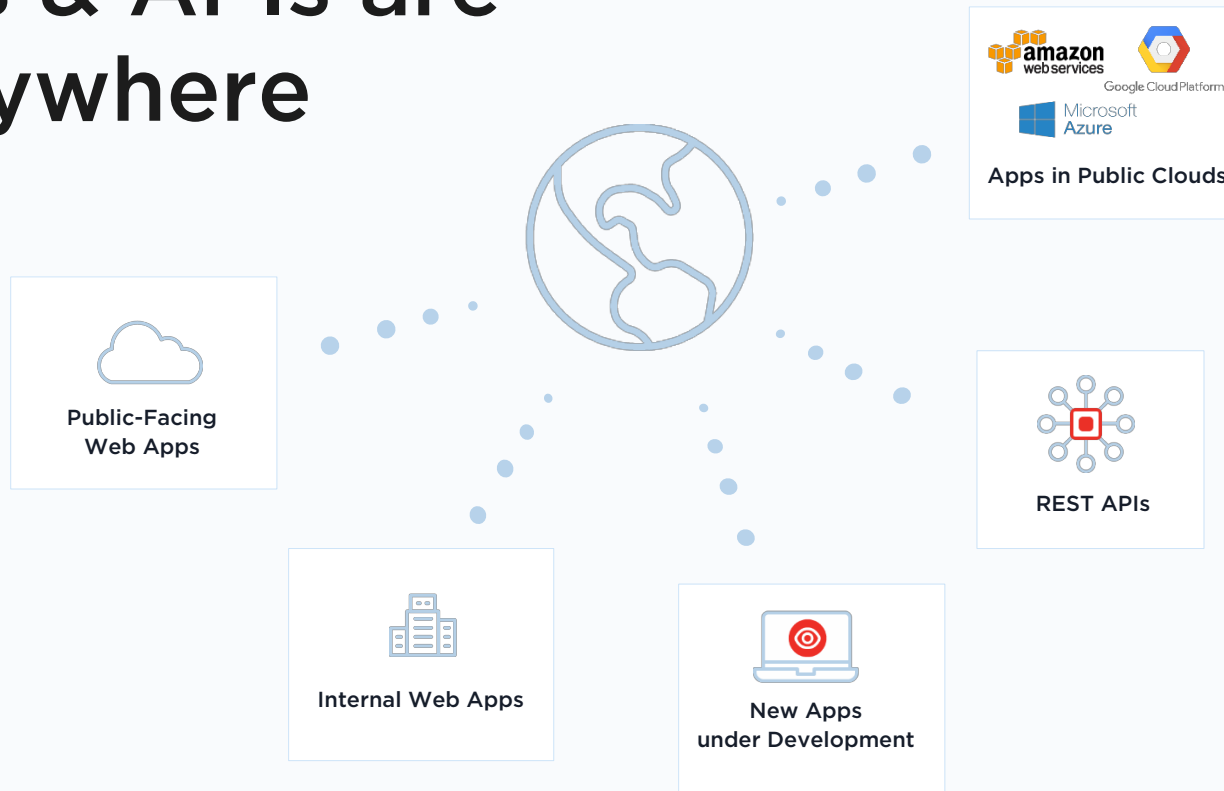
Qualys Web Application Firewall

Review | What's New | Roadmap

Bug Bounty, a new horizon ?

Q&A

# Apps & APIs are Everywhere



# Insecure Apps & APIs are a Problem

Business depends on web applications

Any of them can be a foothold into your organization

Developers are not incentivized for security

Cloud-based apps are easy for developers to deploy

## Web Applications are Being Targeted

- Most common data breach pattern \*
- Top hacking vector \*

<b>U.S. Postal Service (API)</b> .....	2018
<b>Facebook (API)</b> .....	2018
<b>Google+ (API)</b> .....	2018
<b>MyFitnessPal (API?)</b> .....	2017
<b>Equifax</b> .....	2017
<b>Yahoo</b> .....	2016
<b>Ashley Madison</b> .....	2015

\* Source: 2018 Verizon DBIR

# Devops challenges how security is done

Security should start in dev

Security should be a continuous effort

Security is a global concern

CI/CD Tools are powerful

New challenges:

What is in production ?

What server is this app on ?

CI/CD pipe's privileges ?

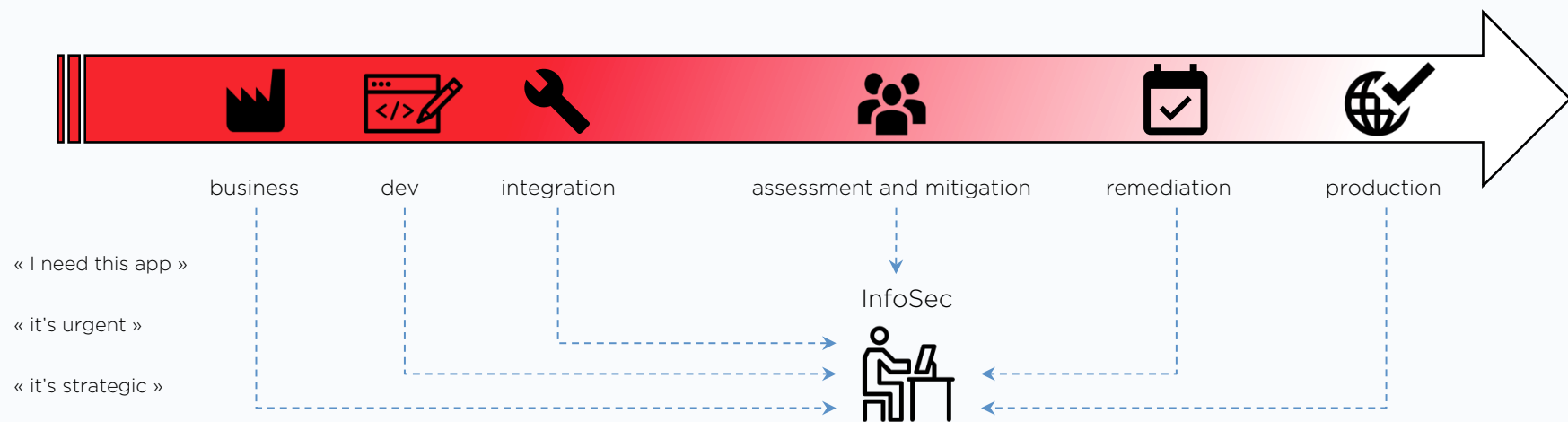
Inefficient/late security

Slowed-down delivery

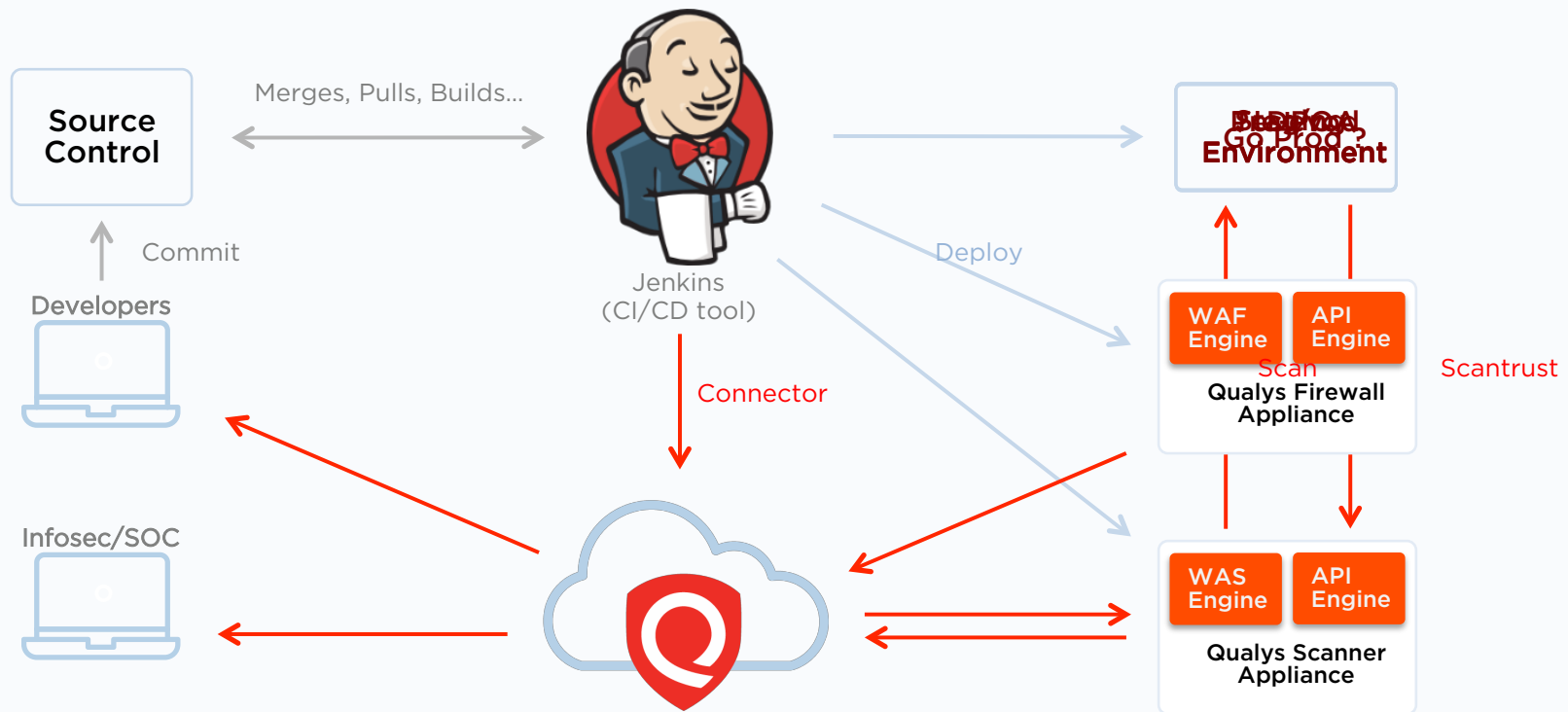
# Web Application Security Built-in

...Not bolted on

# Traditional AppSec Operations



# The way of the DevSecOps





# WAS / WAF Integration: ScanTrust

ScanTrust : Challenge your WAF protection

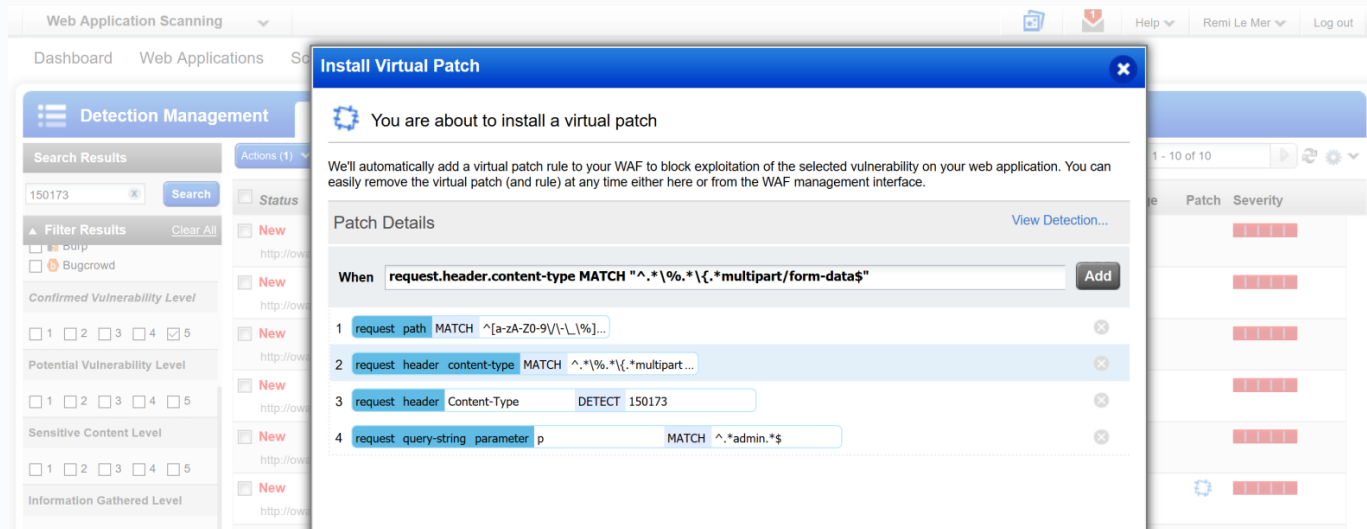
Assess both the application and the policy that protects it

The screenshot displays the ScanTrust Detection Management interface. The top navigation bar includes 'Detection Management', 'Detection List', 'Burp', and 'Bugcrowd'. The main content area shows a table of detected vulnerabilities. The table has columns for Status, QID, Name, Group, Last Detected, Age, Patch, and Severity. The vulnerabilities listed include Blind SQL Injection, Reflected Cross-Site Scripting (XSS) Vulnerabilities, and Browser-Specific Cross-Site Scripting Vulnerabilities. A 'Quick Actions' menu is visible for the selected vulnerability, showing options like View, Ignore, Activate, Install Patch, Remove Patch, Edit Severity, Restore Standard Severity, and External References.

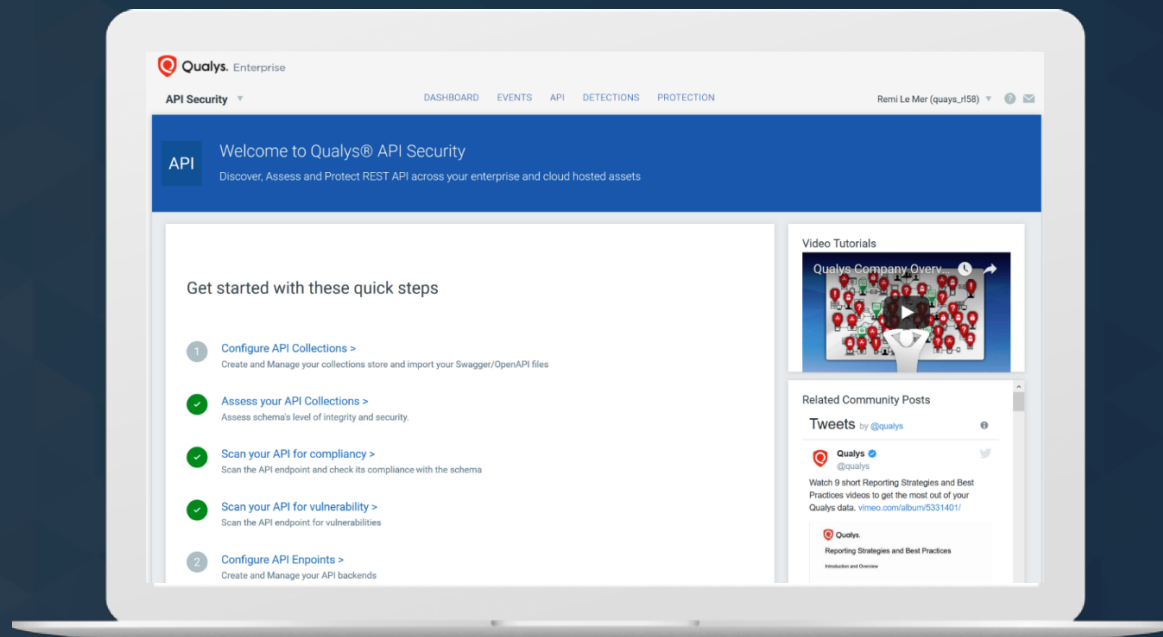
Status	QID	Name	Group	Last Detected	Age	Patch	Severity
Protected	150012	Blind SQL Injection http://waf-demo.qualys.com/bodgeit/login.jsp	SQL	21 Sep 2017	20		High
Protected	150012	Blind SQL Injection http://waf-demo.qualys.com/bodgeit/login.jsp	SQL	21 Sep 2017	20		High
Protected	150001	Reflected Cross-Site Scripting (XSS) Vulnerabilities http://waf-demo.qualys.com/bodgeit/search.jsp	XSS	21 Sep 2017	20		High
Protected	150013	Browser-Specific Cross-Site Scripting Vulnerabilities http://waf-demo.qualys.com/bodgeit/search.jsp	XSS	21 Sep 2017	20		High
Fixed	150001	Reflected Cross-Site Scripting (XSS) Vulnerabilities http://waf-demo.qualys.com/search.jsp	XSS	27 Oct 2016	512		High
New	150001	Reflected Cross-Site Scripting (XSS) Vulnerabilities http://waf-demo.qualys.com/search.jsp	XSS		716		High

# WAS / WAF Integration: Virtual Patch

Virtual Patch : One-click mitigation tool for CISO teams  
Run from within WAS to address confirmed threats



# And Coming in 2019



# Web Application Scanning

## Review

# Qualys WAS

A leading dynamic application security testing (DAST) tool

Delivered via the Qualys Cloud Platform

Identifies app-layer vulnerabilities

- OWASP Top 10

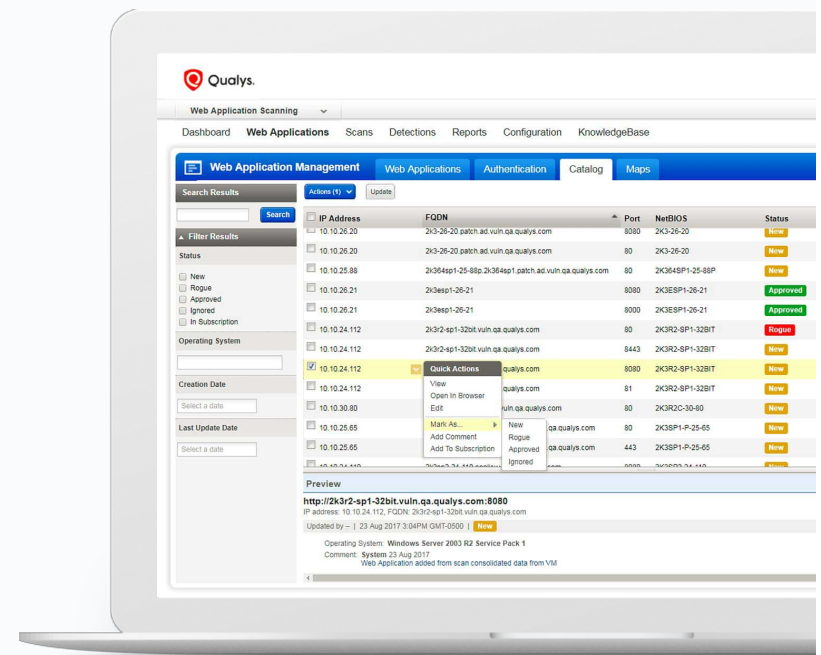
- CWEs

- Web-related CVEs

Includes automated crawling

Supports Selenium scripts

Malware monitoring as a bonus



# Built for the Enterprise



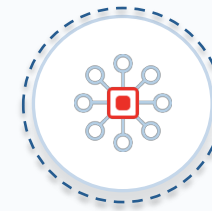
**Web App Discovery**  
Unlimited scans &  
users  
RBAC  
Tagging



**Scheduled scans**  
Ad-hoc, targeted  
scans  
Multi-site scans  
Retest vulnerability  
Scan for malware



**Massive scalability**  
Detection history  
Scheduled reports  
Customizable  
reports  
Swagger support



**Robust API**  
CI/CD integration  
Unique integration  
w/Qualys WAF  
Integration with  
manual pen testing  
tools

# What's New in Qualys WAS

# Scanning REST APIs



[https://  
swagger.io](https://swagger.io)



[https://  
www.openapis.org](https://www.openapis.org)

Swagger is specification that describes a set of REST APIs

Swagger file typically available from dev team

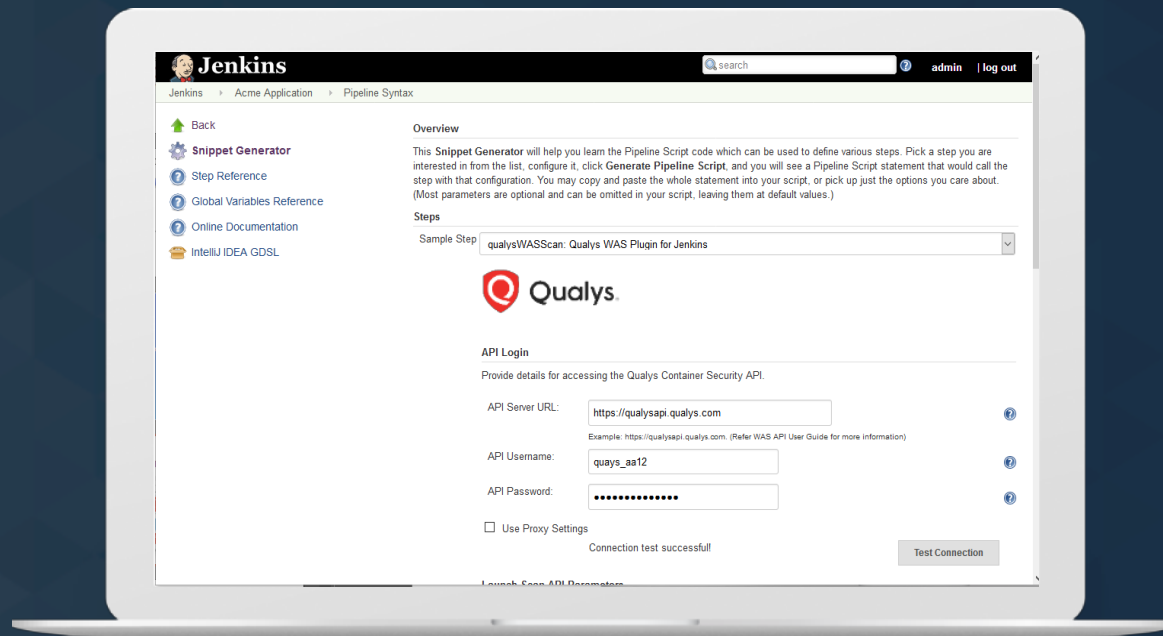
Set Swagger file as target URL in Qualys WAS

API endpoints are automatically tested for vulnerabilities

Swagger v2 JSON format currently supported



# Jenkins Plugin for WAS



# Manual Testing Complements WAS

Dynamic application testing is one piece of the AppSec puzzle  
Manual penetration testing important for your business-critical apps

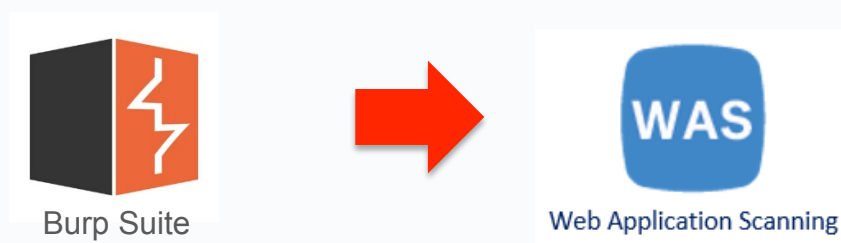
Qualys WAS offers:

- Bugcrowd integration
- Burp Suite integration
- Partnerships with consulting shops

# Bi-directional Integration with Bugcrowd

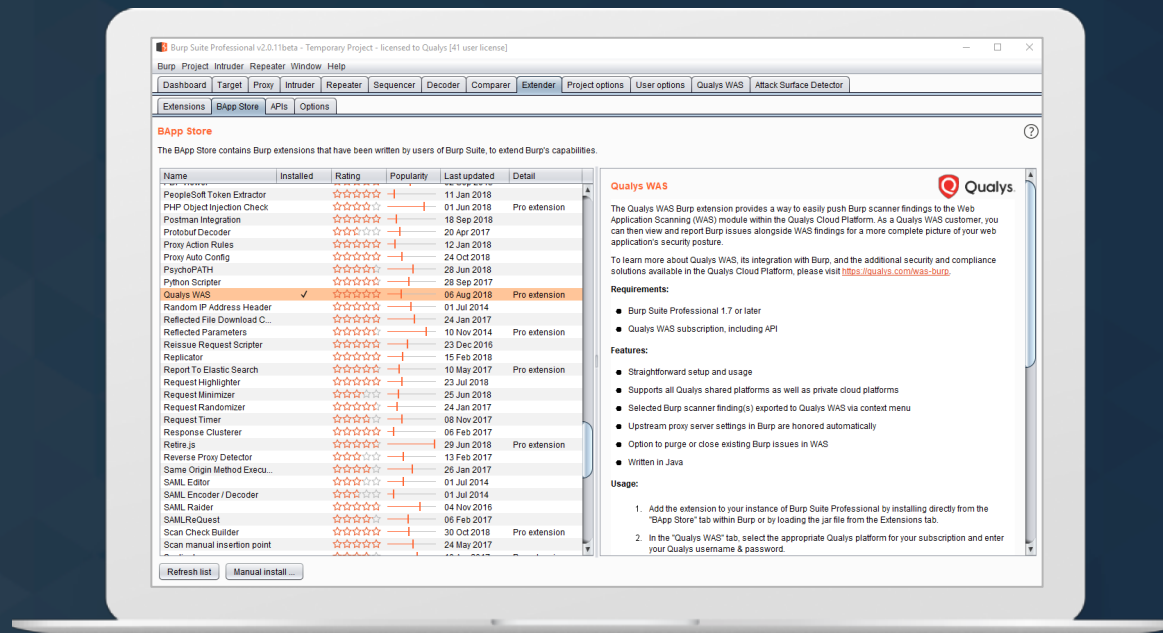


# Qualys WAS Burp Extension

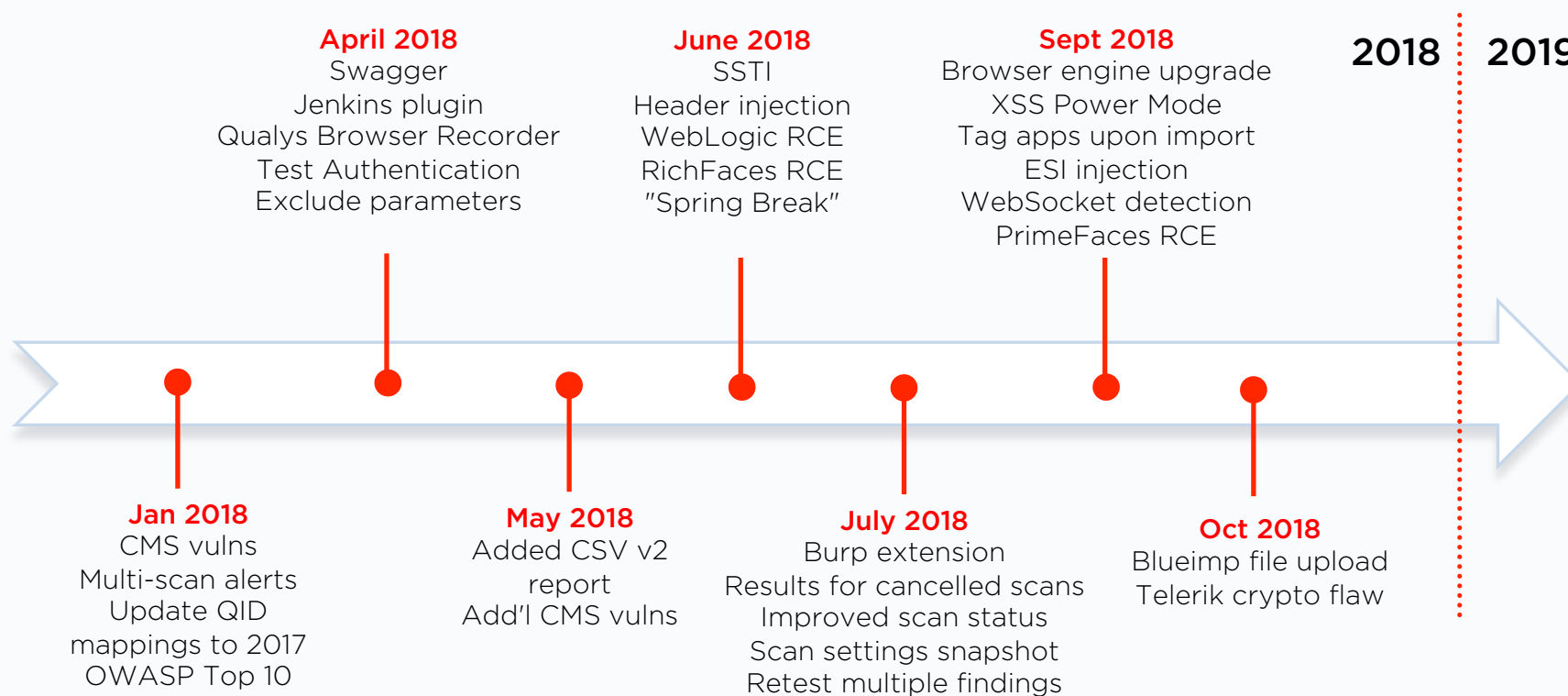


A quick, intuitive way to send Burp-discovered issues into WAS  
Provides centralized viewing/reporting of WAS detections + Burp issues  
Available in Burp's BApp Store

# Qualys WAS Burp extension

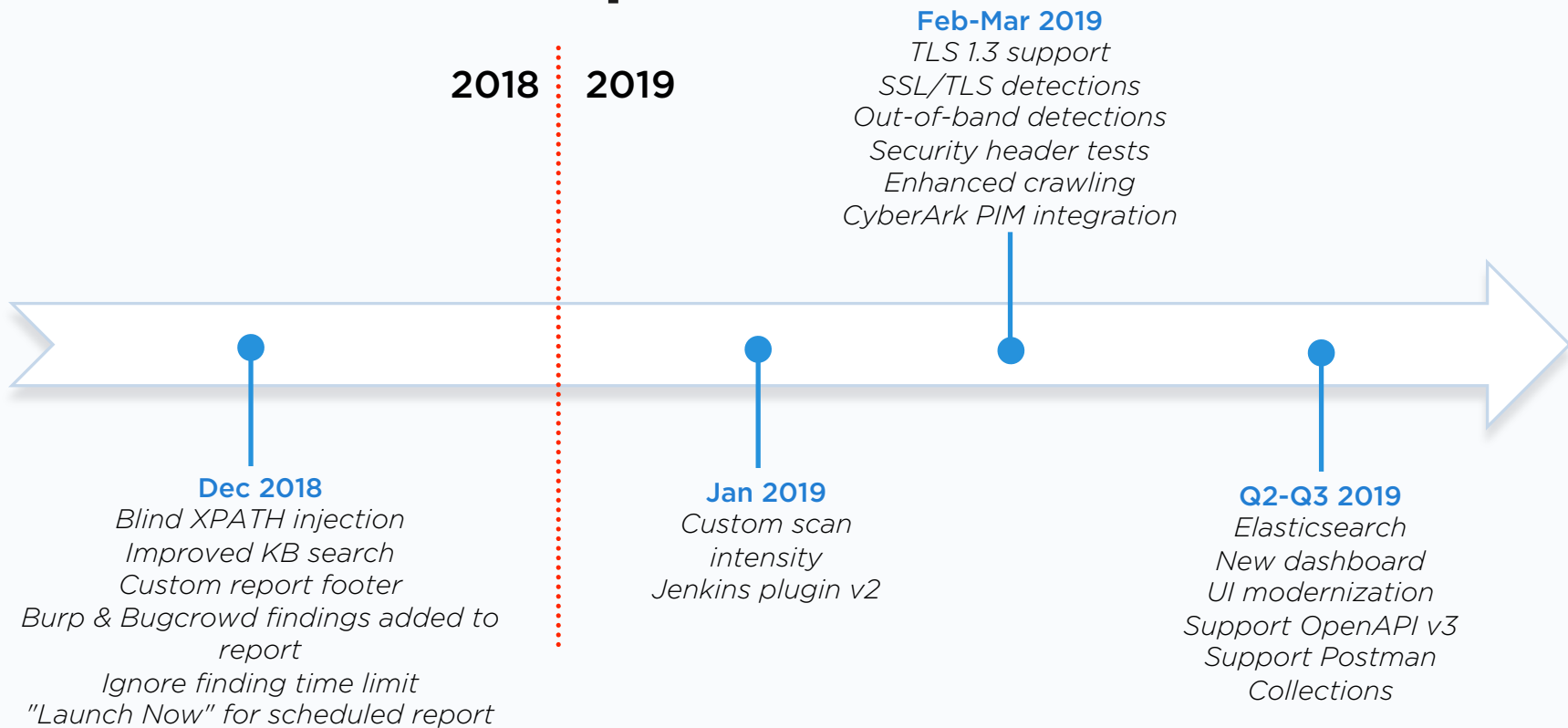


# WAS Enhancements, YTD



# Qualys WAS Roadmap

# WAS Roadmap



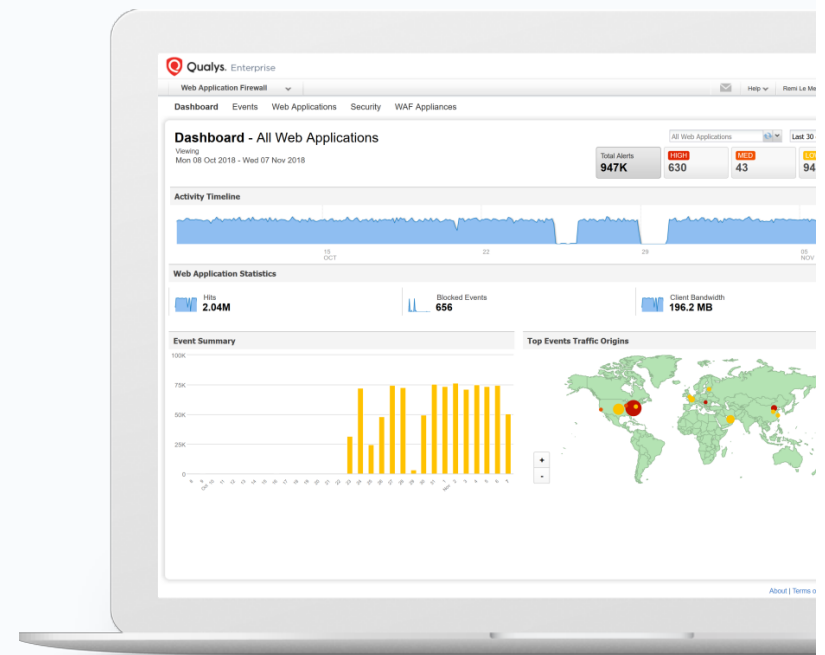


# Web Application Firewall

## Review

# Qualys WAF

Integration with WAS  
Architecture improvements  
Integration with Docker  
Security Improvements  
Roadmap – standalone  
Roadmap – Integrated Suite



# What's New in Qualys WAF

# Supported Platforms

Shared and Private  
Qualys Cloud Platforms

Add New WAF Appliance

Select Virtual Appliance Image

Choose the virtualization platform you want to use to run your WAF appliance on.

Platform	Details
<input checked="" type="radio"/> VMware Standard	VMware virtualization platform
<input type="radio"/> Hyper-V	Microsoft Hyper-V 5.1 virtualization platform
<input type="radio"/> Amazon EC2	Amazon EC2-Classical, Amazon EC2-VPC
<input type="radio"/> Microsoft Azure	Microsoft Azure platform
<input type="radio"/> Google Cloud	Google Cloud platform
<input type="radio"/> Docker	Docker platform

Cancel

PreviousContinue

# WAF Virtual Appliance

Easy and usable Architecture

Virtual Reverse-Proxy

Cluster-able within hybrid topologies

Load-Balancing capabilities

SSL/TLS cipher suite categories



# WAF Improvements

## Virtual Appliance & Container (v1.5.3)

XML/JSON content inspection

Docker Host integration for backend automation

Better performance

Scheduled upgrades

Orchestration via Qualys API

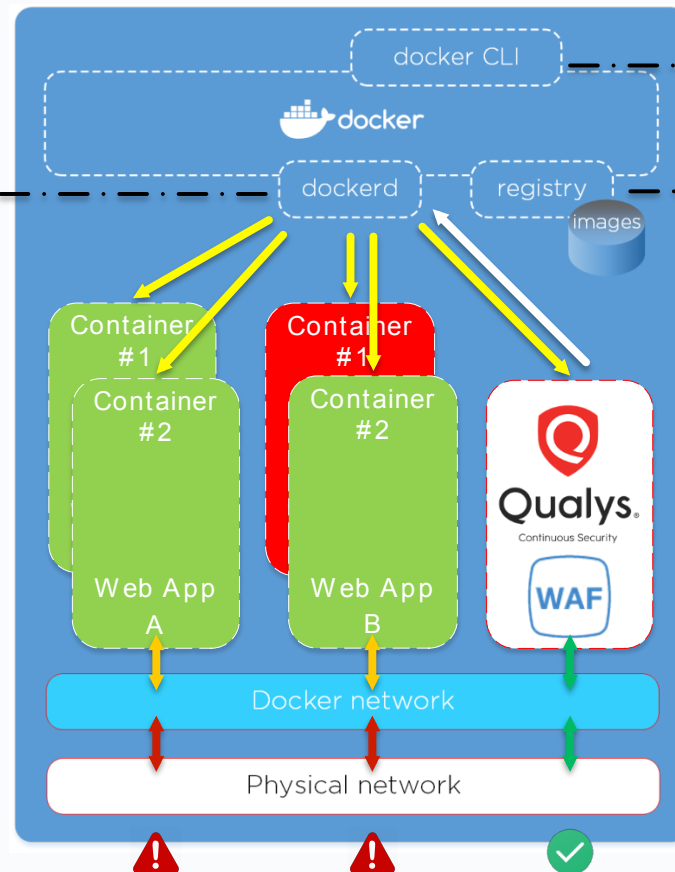


# Docker

## Single Host

### Controls :

- containers (start | stop | delete | inspect)
- networks
- images (pull | push | delete)



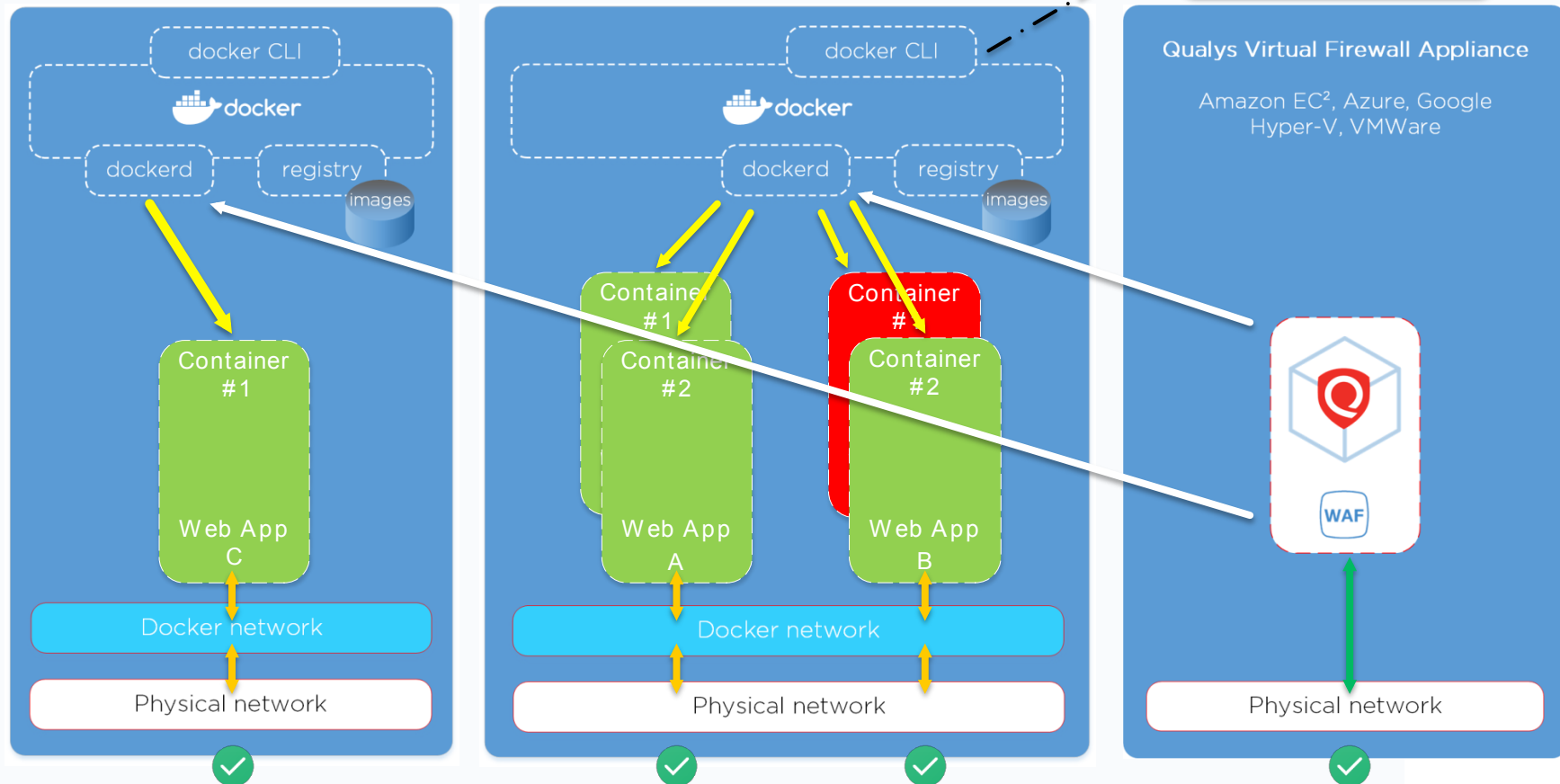
Access to docker services  
via unix sockets

Stores images

# Docker

## Multiple Hosts

Access to docker services via network sockets





# Security Improvements

Custom Rules: write and manage your own filters

- XML/JSON inspection

- Virtual Patches and Event Exceptions

- Latency control

- Rewriting capabilities (headers)

## Qualys Rulesets and Templates

- DAG based inspection, programmable logic

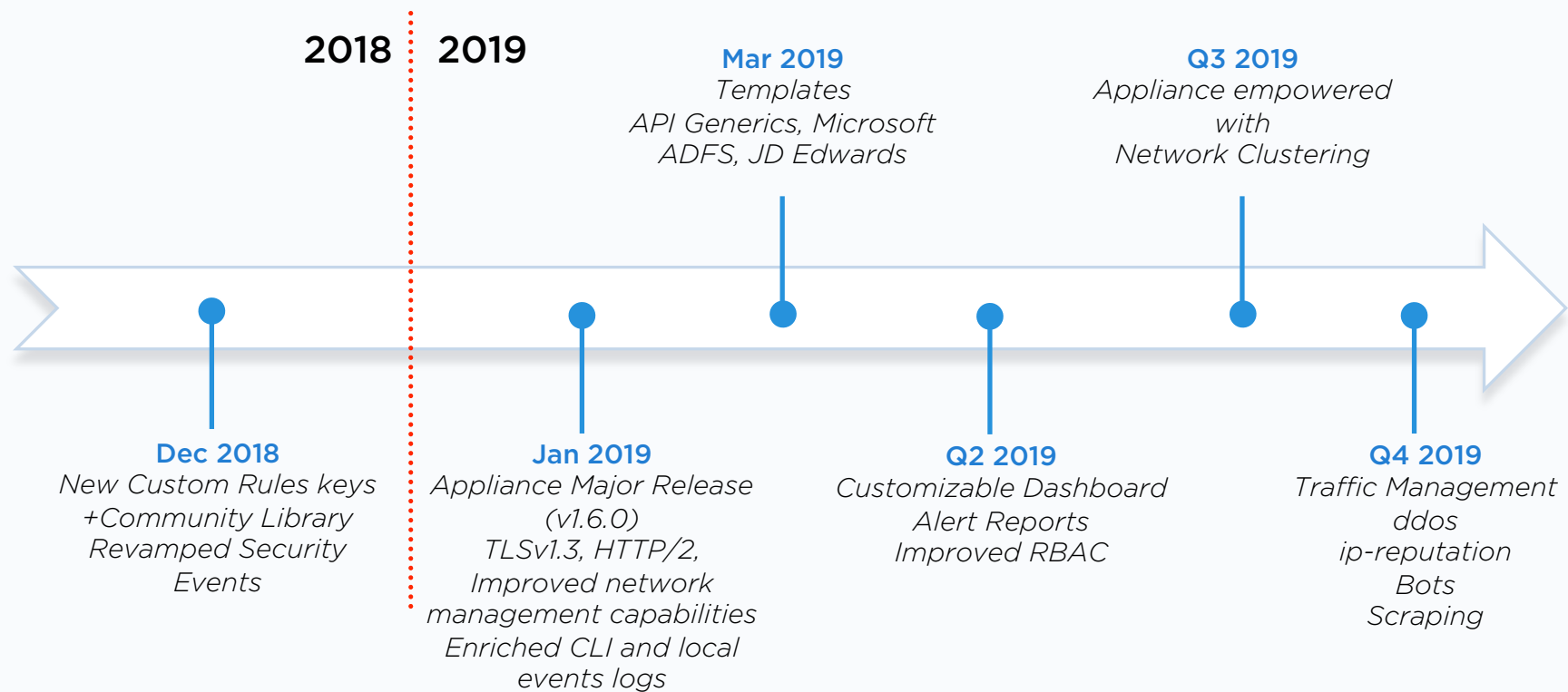
- Drupal 8.0.x, Joomla 3.4.x, Magento 2.5-2.6, Wordpress 4.2.x-4.3.x

- JBoss 4.x-7.x, OWA 2010-2017, Sharepoint 2010-2017, Tomcat 8.0.x

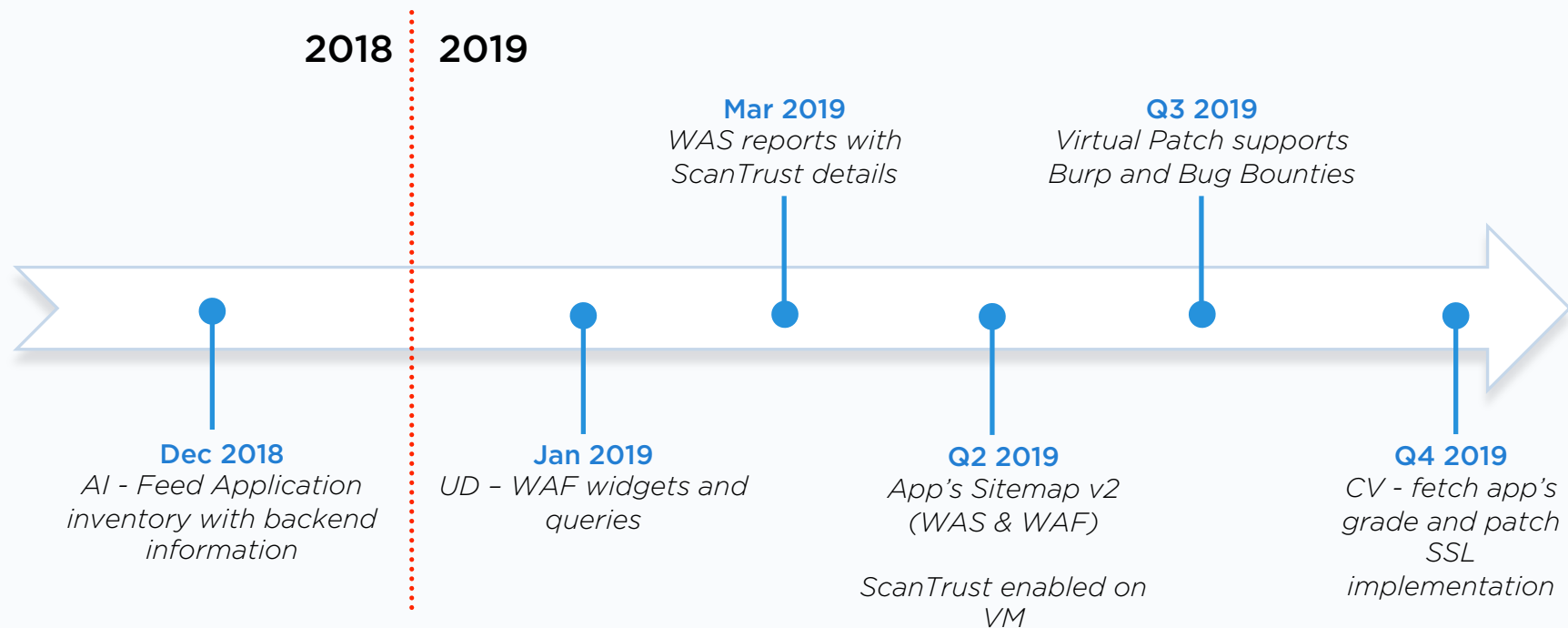
- Qualys Generics for unknown apps

# Qualys WAF Roadmap

# WAF Roadmap - Standalone



# WAF Roadmap - Integrated Suite



# Web Applications & APIs

Intégration et capitalisation des données  
issues d'un programme de Bug Bounty

YES WE H/CK

Romain Lecoivre  
Co-Fondateur & CTO

# Un peu d'histoire...

Le principe du Bug Bounty remonte à 1983, développé à partir de 1995 par Netscape pour permettre à une organisation d'améliorer la sécurité de son système d'information en s'appuyant sur une communauté de chercheurs en vulnérabilités (Crowdsecurity).



**Get a bug if you find a bug.**

Show us a bug in our VRTX® real-time operating system and we'll return the favor. With a bug of your own to show off in your driveway. Bug free.

So, to save up to 12 months of development time, and maybe save a loveable little car from the junkyard, contact us. Call (415) 326-2950, or write Hunter & Ready, Inc., 445 Sherman Avenue, Palo Alto, California 94306.

Describe your application and the microprocessors you're using—28000, 280, 68000, or 8086 family. We'll send you a VRTX evaluation package, including timings for system calls and interrupts. And when you order a VRTX system for your application, we'll include instructions for reporting errors.

But don't feel bad if in a year from now there isn't a bug in your driveway. There isn't one in your operating system either.

**HUNTER & READY**  
**VRTX**  
Operating Systems in Silicon.

\*Call or write for details. But, considering our taste in cars, you might want to accept our offer of \$1,000 cash instead. © 1983 Hunter & Ready, Inc.

# YesWeHack en chiffres

6000+ chercheurs inscrits



120+ nationalités


65% d'Européens

5500+ rapports de vulnérabilités

# Structure d'un rapport

**/ XSS réfléchi sur http://example.com**

 PARTNER PRIVATE PROGRAM 1  2 COMMENTS

 SUBMITTED BY HUNTER\_1 ON 2018-09-24

**REPORT DETAILS**

BUG TYPE	Cross-site Scripting (XSS) - Reflected (CWE-79)
SCOPE	/test
ENDPOINT	http://example.com/?id=
CRITICITY	M
VULNERABLE PART	get-parameter
PART NAME	id
PAYLOAD	"><svg/onload=alert(document.domain)>
APPLICATION FINGERPRINT	php
IP USED	120.12.32.45

CVSS SCORE	CRITICITY
5.4	M
VECTOR STRING CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N	
UPDATE	GIVE 1 BONUS POINT
Quality points	
1 2 3 4 5	



# Intégration ?

Récupération des  
nouveaux rapports de  
vulnérabilités via API

Intégration des rapports  
qualifiés dans un Bug  
Tracker (Bitbucket, git,  
jira, etc.)

## INTEGRATION GITLAB

CLIENT ID:	3_5h075a1bd808s48o8gk448gckskosws4k0080okwks0s4o4soo
CLIENT SECRET:	3qsxrak9016okc8k48kcc84o0g4ooscs4k4oo0o08cw0ksw40s
DOMAIN:	https://internal.dev
REDIRECT URI:	https://internal.dev/get_token

# Intégration ?

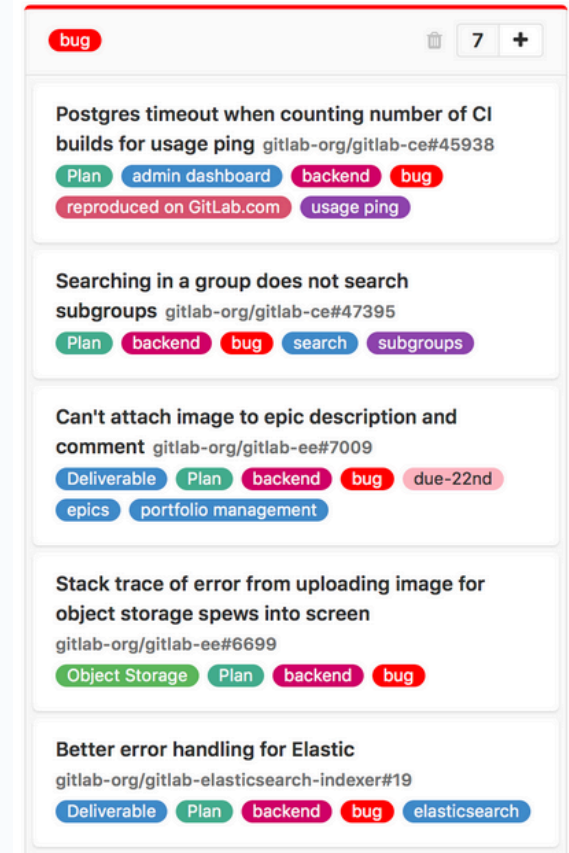
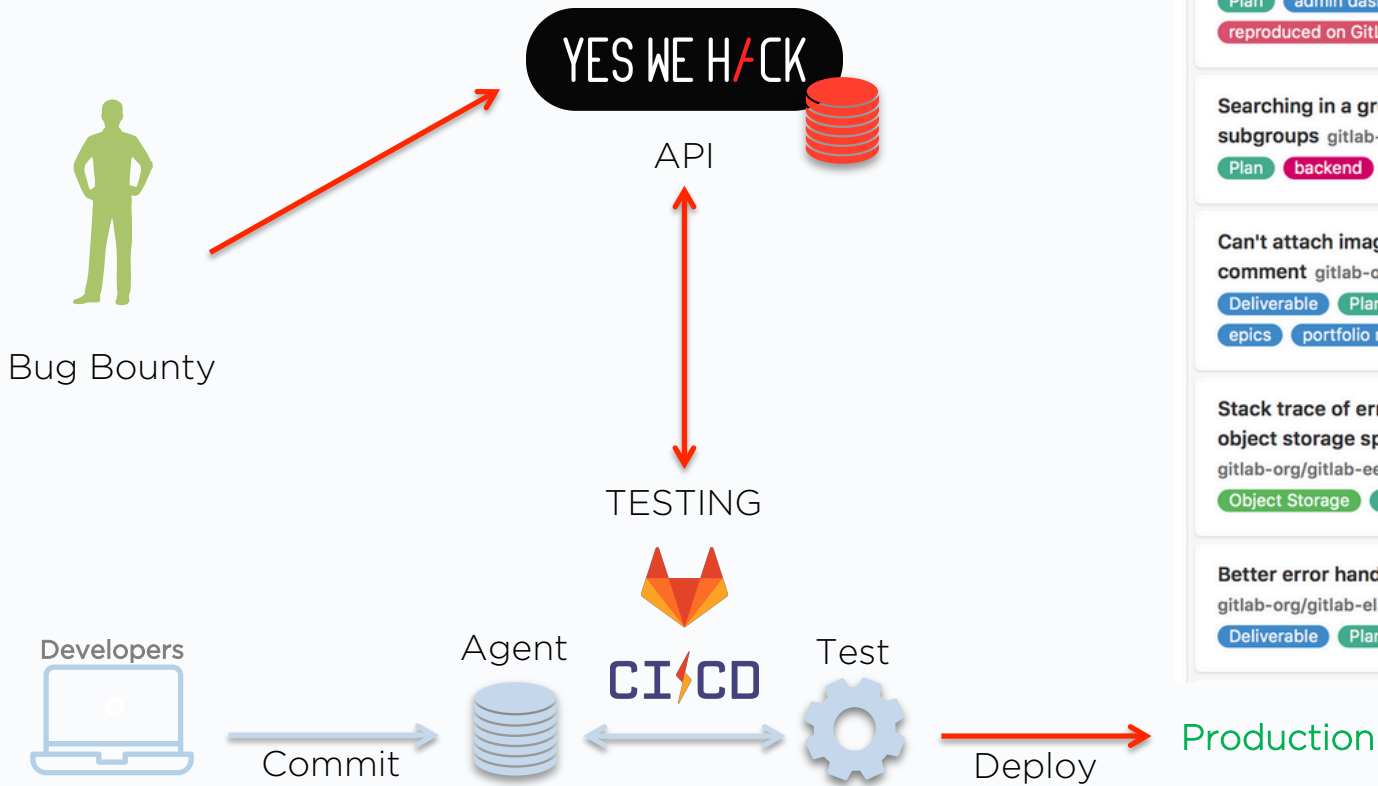
Agent de contrôle intégré dans la CI

Contrôle entre les rapports de vulnérabilités valides et les tests fonctionnels « sécurité »

Non-regression



# Capitalisation ?

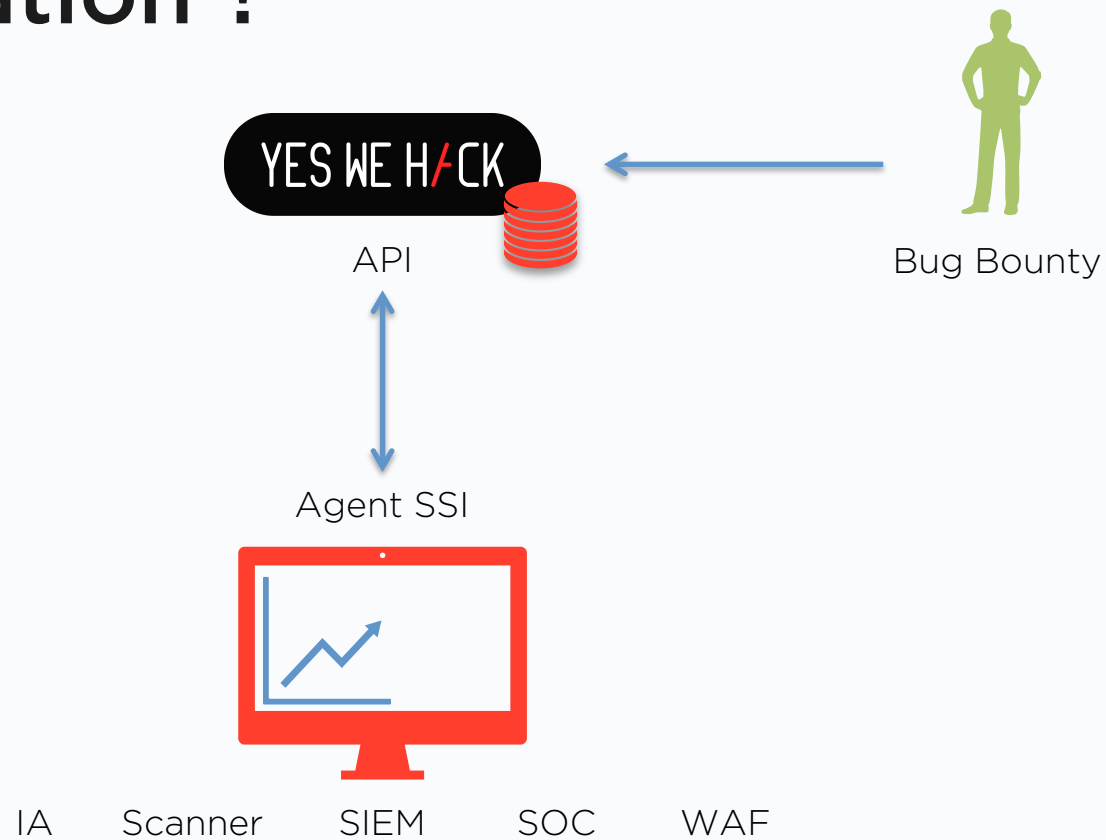


# Capitalisation ?

Agent intégré dans les applications métiers

- IA
- Scanner
- SIEM
- SOC
- WAF

# Capitalisation ?



# Capitalisation ?

The screenshot displays the Qualys Enterprise Web Application Scanning interface. The top navigation bar includes the Qualys logo, 'Enterprise' text, and a dropdown menu for 'Web Application Scanning'. The main navigation bar contains links for 'Dashboard', 'Web Applications', 'Scans', 'Detections', 'Reports', 'Configuration', and 'KnowledgeBase'. The 'Detections' section is active, showing a 'Detection List' with tabs for 'Burp', 'Bugcrowd', and 'YesWeH4ck'. The left sidebar contains a 'Search Results' section with a search bar and a 'Filter Results' section with checkboxes for 'Qualys', 'Burp', 'Bugcrowd', and 'YesWeH4ck'. Below the filters is a 'Confirmed Vulnerability Level' section with checkboxes for levels 1 through 5. The main content area shows a table of detected vulnerabilities. The table has columns for 'Status', 'QID', 'Name', 'Group', 'Last Detected', 'Age', 'Patch', and 'Severity'. Two vulnerabilities are listed, both with a status of 'Active' and a QID of 150046. The first vulnerability is 'Reflected Cross-Site Scripting (XSS) in HTTP Header' with a URL of 'http://demo.qualys.com/vulnerabilities/upload/'. The second vulnerability is also 'Reflected Cross-Site Scripting (XSS) in HTTP Header' with a URL of 'http://demo.qualys.com/vulnerabilities/fi/?page=file3.php'. Both vulnerabilities are in the 'XSS' group, were last detected on '12 Jun 2018', are 185 days old, and have a severity of 5 (indicated by five red bars). The interface also shows a 'Search' button, a 'Clear All' button, and a 'Select a date' dropdown.

Qualys. Enterprise

Web Application Scanning

Dashboard Web Applications Scans **Detections** Reports Configuration KnowledgeBase

Detection Management Detection List Burp Bugcrowd YesWeH4ck

Search Results

Search

Filter Results Clear All

Finding Type

☐ Qualys  
☐ Burp  
☐ Bugcrowd  
☐ YesWeH4ck

Confirmed Vulnerability Level

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

Select a date

Actions (0)

1 - 2 of 2

Status	QID	Name	Group	Last Detected	Age	Patch	Severity
Active	150046	Reflected Cross-Site Scripting (XSS) in HTTP Header http://demo.qualys.com/vulnerabilities/upload/	XSS	12 Jun 2018	185		
Active	150046	Reflected Cross-Site Scripting (XSS) in HTTP Header http://demo.qualys.com/vulnerabilities/fi/?page=file3.php	XSS	12 Jun 2018	185		

# Q&A



QUALYS SECURITY CONFERENCE 2018

# Thank You

**Romain Lecoivre** - [rlecoivre@yeswehack.com](mailto:rlecoivre@yeswehack.com)

**Pierrick Prevert** - [pprevert@qualys.com](mailto:pprevert@qualys.com)

**Remi Le Mer** - [rlemer@qualys.com](mailto:rlemer@qualys.com)